AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
District of Colorado

In the Matter of the Search of A black Apple iPhone 5 cellular telephone and its previously extracted contents, more fully described in Attachment A, attached hereto	)	Case No. 19-sw-5776-NRN

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE "ATTACHMENT A", which is attached to and incorporated in this Application and Affidavit

located in the State and District of Colorado, there is now concealed *(identify the person or describe the property to be seized)*:

SEE "ATTACHMENT B", which is attached to and incorporated in this Application and Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- **X** evidence of a crime;
- **X** contraband, fruits of crime, or other items illegally possessed;
- **X** property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Title 18, U.S.C, § 247	Damage to Religious Property or Obstruction of Persons in the Free Exercise of Religious Beliefs
Title 18, U.S.C, § 249	Hate Crimes
Title 18, U.S.C, § 922(g)(4)	Possession of a Firearm by Person who has been Adjudicated as a Mental Defective or who has been Committed to a Mental Institution

The application is based on these facts:

X Continued on the attached affidavit, which is incorporated by reference.

☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

s/Justin Stern
Applicant's signature

Justin Stern Special Agent
Printed name and title

Sworn to before me and: ☐ signed in my presence.
xx☒ submitted, attested to, and acknowledged by reliable electronic means.

Date: 07/31/2019

N. Reid Neureiter
Judge's signature

City and state: Denver, CO

Magistrate Judge N. Reid Neureiter
Printed name and title

Attachment A

DESCRIPTION OF LOCATION TO BE SEARCHED

The phone and contents to be searched (hereinafter and in Attachment B "Subject Phone") is a black Apple iPhone 5 cellular telephone having International Mobile Equipment Identification number 013426007825476; as well as its previously extracted contents which are contained on a black SanDisk Ultra USB 3.0, 64 gigabyte external thumb drive having serial number 4C530001090628106325. Both the Apple iPhone and external thumb drive are in FBI custody at the FBI Denver Division's Boulder Off-site, located within the Boulder County Sheriff's Office, 5600 Flatiron Parkway, Boulder, Colorado 80301.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

For the Subject Phone described in Attachment A, the following items, that constitute evidence of the commission of, contraband, the fruits of crime, or instrumentalities of violations of: Title 18, United States Code, Section 247, Damage to Religious Property or Obstruction of Persons in the Free Exercise of Religious Beliefs; Title 18, United States Code, Section 249, Hate Crimes; Title 18, United States Code, Section 922(g)(4), Possession of a Firearm by Person who has been Adjudicated as a Mental Defective or who has been Committed to a Mental Institution:

1. Images, videos, visual images and depictions relating to the Subject Offenses and/or showing intent or plans to commit acts of violence, damage religious property or forcefully obstruct free exercise of religion or evincing hatred or bias against individuals or groups of individuals due to their actual or perceived race, color, religion, or national origin;
2. Any and all records, information, notes, software, documents, records or correspondence, in any format and medium relating to the Subject Offenses and/or showing intent or plans to commit acts of violence, damage religious property or forcefully obstruct free exercise of religion or evincing hatred or bias against individuals or groups of individuals due to their actual or perceived race, color, religion, or national origin;
3. Any and all information, notes, documents, records, or correspondence, in any format or medium, concerning Internet activity relating to the Subject Offenses and/or showing intent or plans to commit acts of violence, damage religious property or forcefully obstruct free exercise of religion or evincing hatred or bias against individuals or groups of individuals due to their actual or perceived race, color, religion, or national origin;
4. Any and all address books, names, and lists of names and addresses of individuals who may have been contacted by use of the Subject Phone or by other means for the purpose of committing violations of the Subject Offenses;
5. Any and all information, notes, documents, records, or correspondence, in any format or medium, concerning membership in online groups, clubs, or services that teach, guide, direct, advise or otherwise participate or advocate for violations of the Subject Offenses and/or showing intent to commit acts of violence, damage religious property or forcefully obstruct free exercise of religion or evincing hatred or bias against individuals or groups of individuals due to their actual or perceived race, color, religion, or national origin;
6. Any and all information, records, documents, invoices and materials, in any format or medium, that concern any accounts with an Internet Service Provider pertaining to violations of the Subject Offenses and/or showing intent to commit acts of violence;
7. Any and all information, records, documents, invoices and materials, in any format or medium, that concern e-mail accounts, online storage, or other remote computer storage pertaining to violations of the Subject Offenses and/or showing intent to commit acts of violence, damage religious property or forcefully obstruct free exercise of religion or

evincing hatred or bias against individuals or groups of individuals due to their actual or perceived race, color, religion, or national origin;

8. Records of Internet activity, including Internet Protocol addresses, firewall logs, transactions with Internet hosting providers, co-located computer systems, cloud computing services, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms pertaining to violations of the Subject Offenses and/or showing intent to commit acts of violence, damage religious property or forcefully obstruct free exercise of religion or evincing hatred or bias against individuals or groups of individuals due to their actual or perceived race, color, religion, or national origin;
9. Any and all information, records, documents, invoices and materials, in any format or medium, that concern e-mail accounts, online storage, or other remote computer storage pertaining to violations of the Subject Offenses and/or showing intent to commit acts of violence, damage religious property or forcefully obstruct free exercise of religion or evincing hatred or bias against individuals or groups of individuals due to their actual or perceived race, color, religion, or national origin;
10. Records of Internet activity, including Internet Protocol addresses, firewall logs, transactions with Internet hosting providers, co-located computer systems, cloud computing services, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses pertaining to violations of the Subject Offenses or that show who used, owned, possessed, or controlled the Subject Phone;
11. Any and all information, documents, records, photos, videos, or correspondence, in any format or medium, pertaining to use or ownership of the Subject Phone, or that aid in the identification of persons involved in violations of the Subject Offenses;
12. Any and all information, documents, records, photos, videos, or correspondence, in any format or medium, pertaining to use or ownership of the Subject Phone, or that aid in the identification of persons involved in violations of the Subject Offenses;
13. Credit card information, bills, and payment records pertaining to violations of the Subject Offenses;
14. Descriptions of time, date, locations, items, or events showing or tending to show the commission of, or connecting or tending to connect a person to violations of the Subject Offenses;
15. Evidence of who used, owned, or controlled the Subject Phone to commit or facilitate the commission of the crimes described, or at the time the things described in this warrant were created, edited, or deleted, including photographs, videos, logs, call logs, phonebooks, address books, contacts, IP addresses, registry entries, configuration files, saved usernames and passwords, documents, calendars, browsing history, search terms, metadata, user profiles, e-mail, e-mail contacts, messages (text or voice), instant messaging logs, file structure and correspondence;
16. Evidence of software that may allow others to control the Subject Phone, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security provisions or software designed to detect malicious software or unauthorized use of the device, and evidence of the lack of such malicious software;

17. Evidence of the attachment to the Subject Phone of other storage devices or similar containers for electronic evidence;
18. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Subject Phone;
19. Evidence of how and when the Subject Phone were used or accessed to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
20. The telephone number, ESN number, serial number, and/or SIM card numbers of or contained in the Subject Phone;
21. Passwords, encryption keys, and other access devices that may be necessary to access the Subject Phone; and
22. Contextual information necessary to understand the evidence described in this attachment.

DEFINITIONS

23. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Justin Stern, Special Agent with the Federal Bureau of Investigation ("FBI"), being duly sworn, depose and state under penalty of perjury that the following is true to the best of my information, knowledge and belief.

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the FBI, and have been an agent since December 2004. As a part of my training, I received seventeen weeks of investigative training at the FBI Academy in Quantico, Virginia. Since completing training, I have participated in numerous criminal investigations, which have utilized physical and electronic surveillance, financial analysis, interviews, surreptitious recordings, undercover operations, search warrants, arrests, informants, seizure and analysis of computer information and various other techniques. I have investigated organized crime, drugs, gangs, violent crime, firearms, financial crime, and money laundering. I also investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of the offenses discussed in this affidavit. I am currently assigned in Boulder, Colorado, at an office within the FBI's Denver Division.

2. I make this affidavit in connection with an investigation relating to alleged violations of Title 18, United States Code, Section 247, Damage to Religious Property or Obstruction of Persons in the Free Exercise of Religious Beliefs; Title 18, United States Code, Section 249, Hate Crimes; and Title 18, United States Code, Section 922(g)(4), Possession of a Firearm by Person who has been Adjudicated as a Mental Defective or who has been Committed to a Mental Institution (hereinafter "Subject Offenses"). This affidavit is made in support of an application for a search warrant for an Apple iPhone 5 cellular telephone and its previously

extracted contents (hereinafter "Subject Phone"), described herein and in Attachment A, with items to be seized described in Attachment B.

3. As the primary Case Agent for this investigation, I am familiar with the facts of the case. The facts set forth in this affidavit are based on my personal knowledge as the investigation's Case Agent; knowledge obtained from other individuals including law enforcement personnel; and my review of reports and other evidence. The information contained within this affidavit does not represent every fact learned by law enforcement during the course of the investigation but includes information sufficient to establish probable cause for the requested search warrant.

4. Based on the information below, I submit there is probable cause to believe that fruits, evidence and instrumentalities of the Subject Offenses as described in Attachment B, will be located on the Subject Phone, as described in Attachment A.

RELEVANT STATUTES

5. This investigation concerns alleged violations of Title 18, United States Code, Sections 247, 249, and 922(g)(4). Section 247 prohibits intentionally defacing, damaging, or destroying any religious real property because of the religious character of the property or intentionally obstructing, by force or threat of force, any person in the enjoyment of that person's free exercise of religious beliefs. Section 249 prohibits willfully causing bodily injury to any person because of their actual or perceived race, color, religion, national origin, sexual orientation, gender identity, or disability under certain circumstances affecting interstate or foreign commerce. Section 922(g)(4) prohibits the possession of a firearm by a person who has previously been adjudicated a mental defective or who has been committed to a mental institution.

DEFINITIONS

6. The following definitions apply to this affidavit and Attachment B.

7. "IP Address" means Internet Protocol address, which is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

8. "Internet" means a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

9. In this affidavit, the terms "computers" or "digital storage media" or "digital storage devices" may be used interchangeably, and are intended to include any physical object upon which computer data can be recorded as well as all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices capable of performing logical, arithmetic, or storage functions, including desktop and laptop computers, mobile phones, tablets, server computers, game consoles, network hardware, hard disk drives, RAM, floppy disks, flash memory, CDs, DVDs, and other magnetic or optical storage media.

IDENTIFICATION OF THE DEVICE TO BE SEARCHED

10. The Subject Phone is a black Apple iPhone 5 cellular telephone and its previously extracted contents which are contained on an external thumb drive, currently in FBI custody and

more particularly described in Attachment A. In my training and experience, I know that the Subject Phone has been stored in a manner in which the contents are, to the extent material to this investigation, in substantially the same state as they were when the phone first came into the possession of the FBI.

INVESTIGATION

Execution of Federal Search Warrant on an Apple iPhone

11. On July 25, 2019, United States Magistrate Judge Kristen L. Mix authorized a search warrant (*see* 19-SW-5759-KLM) for the contents of the Apple iPhone (hereinafter Subject Phone) for evidence, fruits and instrumentalities of violations of: Title 18, United States Code, Section 2252, Certain Activities Relating to Material Involving the Sexual Exploitation of Minors; Title 18, United States Code, Section 2252A, Certain Activities Relating to Material Constituting or Containing Child Pornography. I incorporate the affidavit in support of that search warrant here by reference. [1]

12. On July 26, 2019, I executed the search warrant. Thereafter, with the assistance of an FBI Computer Scientist, I began identifying and analyzing items and information on the phone, as authorized by the search warrant. During the course of my search of the Subject Phone, I found, in plain view, evidence of the Subject Offenses. This affidavit requests the Court's authorization to continue searching the Subject Phone for such items.

[1] The July 25, 2019 affidavit states that the Subject Phone was recovered on May 30, 2019. On July 27, 2019, Officer Hartkopp advised me that his report mistakenly identified May 30, 2019, as the date RTD Employee 1 recovered the Apple iPhone. RTD Employee 1 actually recovered the Apple iPhone on May 31, 2019, approximately one hour before Officer Hartkopp responded to the call during the early hours of June 1, 2019.

13. As detailed in the affidavit in support of July 25, 2019 search warrant, Boulder Police Department (BPD) previously searched the Subject Phone. I have intentionally omitted any evidence or information derived from BPD's search from the affidavits. However, I advise the Court that prior to my execution of the federal search warrant, BPD Detective Owen McKinney advised me that he found evidence of the Subject Offenses during his search and specifically alerted me to some of same evidence I later saw in plain view during my execution of the federal search warrant.

Evidence Identifying Wesley D. Gilreath as the Owner/User of the Apple iPhone

14. Among other things, my analysis of the Subject Phone identified the cellular telephone as: an Apple iPhone 5; having last used mobile telephone number 1-317-777-1511; and having Apple identification "videomagazinist@gmail.com." The name "Wes Gilreath" was noted in the telephone's contacts having email address videomagazinist@gmail.com. An email retrieved from the Apple iPhone was sent from videomagazinist@gmail.com on April 7, 2019, at approximately 3:29:16 a.m.

15. Messaging information on the Apple iPhone also identifies Wesley D. Gilreath (GILREATH) as its owner. On November 9, 2018, at approximately 4:07:24 p.m., telephone number 1-317-777-1511 sent an "iMessage" to telephone number 1-317-407-3515, identified as "Dad." The message reads [verbatim]: "I don't know what this is about and it is not okay for me to get random charges to my debit card." A photograph is attached to the message. The photograph is titled "IMG_0008.JPG." I have reviewed the photograph, which appears to be a healthcare statement from Kaiser Permanente, titled "Premium Bill." The statement is addressed to: Wesley David Gilreath; 3605 Table Mesa Dr Apt M256, Boulder, Colorado 80305-5858. The premium due date is October 31, 2018.

16. Additional messaging on the Subject Phone between the user of the phone and "Dad" appear to reference the FBI interview of GILREATH discussed in the next section and further serve to identify GILREATH as the user of the Subject Phone.

17. On July 22, 2019, I caused a query of a Colorado Division of Motor Vehicles database for information concerning GILREATH. The results showed Colorado driver's license number 17134851 was issued to GILREATH on May 24, 2019. The license identified GILREATH's full name as Wesley David Gilreath. The address listed on the license is 3605 Table Mesa Dr Apartment M256, Boulder, Colorado 80305-5858. GILREATH's birth year is listed as 1990.

FBI Interview of GILREATH

18. During the course of my investigation, I learned that the FBI has had prior contact with GILREATH. Specifically, on January 24, 2019, FBI Task Force Officer (TFO) Eric Miller interviewed Wesley D. Gilreath in Boulder, Colorado, after receiving information that GILREATH had posted a "Montana Hunting Guide" online. The FBI identified GILREATH as the poster after receiving a tip advising that a then unknown entity was posting "hunting guides" concerning: Jews; Muslims; Bureau of Land Management and Montana National Guard facilities; and a refugee center. I am aware that FBI investigators understand some such "hunting guides" to contain information that may be used to violently target individuals or entities with belief systems, identities, ethnicities, religions, political views or other matters antithetical to their own.

19. GILREATH's attorney, Jason Savela, was present for the FBI interview. During the interview, GILREATH told TFO Miller that although GILREATH did not label himself a white supremacist, GILREATH wanted the white race to win at life. GILREATH described

winning as having money and property, while not allowing others to take those resources. GILREATH confirmed that GILREATH posted the Montana Hunting Guide online. He stated that he provided the information hoping that people would protest at the listed locations. He explained that he listed the particular locations refugees are in the United States illegally and are taking resources, many people do not like Muslims, the Bureau of Land Management takes land from people and the Bundy's won their court case, and Jews are responsible for the refugee crisis.

GILREATH is a Prohibited Person and Recently Attempted to Obtain a Firearm

20. On July 23, 2019, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) Special Agent John Zavodsky provided information to FBI Special Agent Marisa Budwick concerning GILREATH's attempted purchase of a firearm at the Gunsport firearms shop in Boulder on May 24, 2019. GILREATH completed ATF form 4473 as part of the attempted purchase. I have reviewed a copy of GILREATH's completed form 4473. GILREATH listed his residence as 3605 Table Mesa Drive M256, Boulder, Colorado 80305. GILREATH presented identification was Colorado driver's license number 17134851. Handwritten on the top of the form is the note: "Denied 5-24-19."

21. Section A of the form is titled "Must be Completed by Transferee/Buyer." Question 11f asks: "Have you ever been adjudicated as a mental defective OR have you ever been committed to a mental institution?" In response to this question, the "no" box is checked. The form was signed by GILREATH and dated May 24, 2019.

22. According to Agent Zavodsky, GILREATH's attempted purchase of a firearm on May 24, 2019, was denied because he was previously adjudicated as a mental defective or

committed to a mental institution on March 21, 2016, pursuant to Boulder County Court, case number 2016-MH-129.

23. Attached to the form 4473 is another document titled "Appeal of Firearm Denial." The form contains GILREATH's identifying information and instructions on how to appeal a denial of a firearms transfer background check. The National Instant Criminal Background Check System (identified on the form by the acronym NICS) number identified on the appeal was 1010D3PVZ. On July 29, 2019, I called the Colorado Bureau of Investigation (CBI) Firearm Instacheck Unit for information concerning NICS number 1010D3PVZ. CBI told me that NICS number 1010D3PVZ regarded GILREATH's determination as mentally defective and that the record was created/updated on March 21, 2016.

24. Review of the Subject Phone reveals that on May 24, 2019, at approximately 2:48:33 p.m., GILREATH sent the following iMessage to "Dad": "You've permanently ruined my ability to buy a gun in CO and other states."

Evidence of the Subject Offenses in Plain View

25. During the course of my review of the Subject Phone for evidence as authorized by the July 25, 2019 federal search warrant, I observed the following evidence of the Subject Offenses in plain view.

26. I reviewed a video saved on the Subject Phone that appears to be the actual video footage of the gunman shooting and killing fifty-one people at mosques in Christchurch, New Zealand on March 15, 2019. The file name of this video is "IMG_2424.mp4" and it was saved to the Subject Phone on March 15, 2019, at approximately 12:06:47 a.m. I reviewed the content of this video, among others, to determine whether it contained any evidence of child pornography. I know from my training and experience that in order to search for evidence of

child pornography, investigators must actually access and view video files, even if the still image created by the forensic tool used to extract data from the Subject Phone does not appear to depict child pornography, because other portions of the video may nonetheless contain child pornography. I also know that individuals who possess child pornography sometimes intentionally mislabel or save such content with misleading names to avoid discovery.

27. In the "notes" section of the Subject Phone I observed the following. A note was present that appeared to reference Oklahoma City Federal Building bomber Timothy McVeigh and an interest in C4 explosives. The note was created on November 22, 2018 at approximately 10:43:29 p.m. and modified on April 24, 2019 at approximately 4:50:41 a.m. The title of the note was [verbatim]: "Tim's favorite reading[.]" The summary of the note was [verbatim]: "Homemade C-4[.]" The body of the note contains the following entries, among others: "Homemade C-4" and "Improvised Munitions."' I reviewed the content of this note, among others, during my execution of the July 25th search warrant because I know from my training and experience that the title and summary of a note does not always accurately reflect its contents and that it is not possible to discern whether a note is evidence of child pornography without reviewing its content.

28. I observed evidence that, at the following dates and times, the Subject Phone's browser visited websites with the following titles:

- On May 24, 2019, at approximately 4:13:04 a.m.: "9mm small pistol – Google Search."
- On May 24, 2019, at approximately 4:10:05 a.m.: "best small 380 pistol – Google Search."
- On May 28, 2019, at approximately 9:28:26 p.m.: "Black Death Jewish persecutions – Wikipedia."

- On May 28, 2019, at approximately 3:05:18 p.m.: "Browse Mosque Locations – USA Mosques/Masjids."
- On May 28, 2019, at approximately 3:26:08 p.m.: "Home – United Nations Association of Boulder County."
- On May 29, 2019, at approximately 12:51:53 p.m.: "Israel Did 911 - YouTube."
- On May 28, 2019, at approximately 4:48:39 p.m.: "jewish conspiracy exposed – YouTube."
- On May 28, 2019 at approximately 3:00:16 p.m.: "Mosques and Islamic Schools in Denver Metro, Colorado – Salatomatic – your guide to mosques and Islamic schools."
- On May 28, 2019, at approximately 3:49:16 p.m.: "Synagogues in Boulder, United States."
- On May 28, 2019, at approximately 3:49:02 p.m.: "Synagogues in Colorado, United States."
- On May 29, 2019, at approximately 10:20:38 p.m.: "Timothy McVeigh – YouTube."
- On May 28, 2019, at approximately 9:28:15 p.m.: "Well poisoning – Wikipedia."
- On May 19, 2019, at approximately 6:24:04 a.m.: "uranium thorium fusion bomb."

I viewed the titles of these websites while reviewing the full list of records of visited websites extracted by the forensic tool, consistent with my training and experience, to search for evidence of websites that may contain child pornography.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

29. A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other

wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet including websites, social media sites, bulletin boards, file sharing, and other Internet sites. Wireless telephones often have a subscriber identity module or subscriber identification module ("SIM"), which is an integrated circuit that securely stores the International Mobile Subscriber Identity ("IMSI") and the related key used to identify and authenticate subscribers on mobile telephone devices. A SIM is embedded into a removable "SIM card," which can be transferred between different mobile devices. A SIM card contains a unique serial number ("ICCID"), IMSI, security authentication and ciphering information, temporary information related to the local network, a list of the services to which the user has access, and certain passwords. Most SIM cards will also store certain usage data, such as call history, text ("SMS") messages, and phone book contacts. Wireless telephones may also be "smartphones," such that they operate as personal computers capable of accessing the Internet. They may also include GPS technology for determining the location of the device. Such telephones may also contain removable storage media, such as a flash card—such devices can store any digital data, and can have the capacity to store many gigabytes of data. Some cellular telephones also have software, giving them the same capabilities as personal computers including accessing and editing word processing documents, spreadsheets, and presentations.

Some cellular telephones also operate as a "tablet," or mobile computer, and can contain software programs called applications. Those programs can perform different functions and save data associated with those functions, including use associated with the Internet.

30. Based on my experience, as well as information imparted to me by other law enforcement officers, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, that is, in space on the storage medium that is not currently being used by an active file for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

31. Also, again based on my experience, as well as information imparted to me by other law enforcement officers, I know that wholly apart from user-generated files, computer storage media contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, virtual memory "swap" or paging files, and shadow copies of previous versions of systems or files, or paging files. Computer users typically do not erase or delete this evidence because special software is typically required for that task. However, it is technically possible to

delete this information. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted, edited, moved, or show a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

32. As further described in Attachment B, this application seeks permission to locate not only digital files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how devices were used, why they were used, the purpose of their use, and the purposes to which they were put, who used them, the state of mind of the user(s), and when they were used.

33. Information or files related to the crimes described herein are often obtained from the Internet or the cellular data networks using application software which often leaves files, logs or file remnants which would tend to show the identity of the person engaging in the conduct as well as the method of location or creation of the images, search terms used, exchange, transfer, distribution, possession or origin of the files. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them. Thus, the ability to retrieve residue of an electronic file from a hard

drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

34. "User attribution" evidence can also be found on a computer and is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, videos, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time. For example, I know from experience, as well as information imparted to me by other law enforcement officers, that persons involved in offenses such as the subject offenses communicate with others through correspondence or other documents which could tend to identify persons involved in such offenses as well as provide evidence of a person's intent and/or motive. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

35. I know from experience, as well as information imparted to me by other law enforcement officers, that digital software or hardware exists that allows persons to share digital access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address. Examination of these items can reveal information about the authorized or unauthorized use of Internet connection at the residence.

36. Searching computer(s) for the evidence described in the attachment may require a range of data analysis techniques. For example, information regarding user attribution or

Internet use is located in various operating system log files that are not easily located or reviewed. Or, a person engaged in criminal activity will attempt to conceal evidence of the activity by "hiding" files or giving them deceptive names. As explained above, because the warrant calls for records of how a computer has been used, what it has been used for, and who has used it, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this premises for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use a multitude of techniques, both on and off-scene, including more thorough techniques.

37. Furthermore, because there is probable cause to believe that computer(s) and storage devices are all instrumentalities of crimes involving child exploitation, they should all be seized as such.

38. Based upon my experience, as well as information imparted to me by other law enforcement officers, I know that a thorough search for information stored in digital storage media requires a variety of techniques that often includes both on-site seizure and search as well as a more thorough review off-site review in a controlled environment. This variety of techniques is required, and often law enforcement officers must seize most or all storage media to be searched on-scene and/or later in a controlled environment. These techniques are often

necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction.

39. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include off-site techniques since it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined off-site and in a controlled environment. This is true because of the following:

a. The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how, when and why a computer has been used, by whom, what it has been used for, requires considerable time, and taking that much time on premises could be unreasonable. Also, because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a "booby-trap"), the controlled environment of a laboratory may be essential to its complete and accurate analysis. Searching for and attempting to recover any deleted, hidden, or encrypted data may be required to determine whether data falls within the list of items to be seized as set forth herein (for example, data that is encrypted and unreadable may not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of child exploitation offenses).

b. The volume of evidence and time required for an examination. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order

with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Reviewing information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

c. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

e. Need to review evidence over time and to maintain entirety of evidence. I recognize the prudence requisite in reviewing and preserving, in its original form, only such records applicable to the violations of law described in this affidavit and in Attachment B in order to prevent unnecessary invasion of privacy and overbroad searches. I submit it would be impractical and infeasible for the Government to review the mirrored images of digital devices that are copied as a result of a search warrant issued pursuant to this Application during a single analysis. I have learned through practical experience that various pieces of evidence retrieved from digital devices in investigations often have unknown probative value and linkage to other pieces of evidence in the investigation until they are considered within the fluid, active, and ongoing investigation of the whole as it develops. In other words, the weight of each individual piece of the data fluctuates based upon additional investigative measures undertaken, other documents under review and incorporation of evidence into a consolidated whole. Analysis is content-relational, and the importance of any associated data may grow whenever further analysis is performed. The full scope and meaning of the whole of the data is lost if each piece is observed individually, and not in sum. Due to the interrelation and correlation between pieces of an investigation as that investigation continues, looking at one piece of information may lose its full evidentiary value if it is related to another piece of information, yet its complement is not preserved along with the original. In the past, I have reviewed activity and data on digital devices pursuant to search warrants in the course of ongoing criminal investigations. I have learned from that experience, as well as

other investigative efforts, that multiple reviews of the data at different times is necessary to understand the full value of the information contained therein, and to determine whether it is within the scope of the items sought in Attachment B. In order to obtain the full picture and meaning of the data from the information sought in Attachments A and B of this application, the Government would need to maintain access to all of the resultant data, as the completeness and potential of probative value of the data must be assessed within the full scope of the investigation. As such, I respectfully request the ability to maintain the whole of the data obtained as a result of the search warrant, and to maintain and to review the data in the control and custody of the Government and law enforcement at times deemed necessary during the investigation, rather than minimize the content to certain communications deemed important at one time. As with all evidence, the Government will maintain the evidence and mirror images of the evidence in its custody and control, without alteration, amendment, or access by persons unrelated to the investigation.

CONCLUSION

40. Based on the foregoing, probable cause exists to believe that that inside the Subject Phone (described on Attachment A), will be found evidence, fruits, and instrumentalities of a violation of Title 18, United States Code, Sections 247, 249, and 922(g)(4) (described on Attachment B)

41. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items described in Attachment A for the items listed in Attachment B.

I declare under the penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Respectfully Submitted,

s/ Justin Stern

Justin Stern
Special Agent
Federal Bureau of Investigation

SUBSCRIBED and SWORN before me this 31st day of July 2019
(by reliable electronic means)

N. Reid Neureiter

UNITED STATES MAGISTRATE JUDGE

Application for search warrant was reviewed and is submitted by Julia Martinez, Assistant United States Attorney.